

AMENDMENTS TO THE CLAIMS

The listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of the Claims:

1. (Currently Amended) A communication device for verifying whether application data is valid in order to determine whether to execute the application data on the communication device, the verification of the application data using a first file, a second file, and a third file, the first file comprising the application data, the second file comprising application validity data used to verify validity of the application data in the first file and containing data indicating a location where a program, which is contained in the first file and run in the communication device, is stored, the first file, second file, and the third file being separate from one another, the third file comprising second file validity data calculated with a one-way function and used to verify the second file, the communication device comprising:

a receiver for receiving the first file, second file, and third file;

at least one processor for:

generating a second file calculated value using the one-way function, at least a part of the second file being input to the one-way function to generate the second file calculated value;

comparing the second file calculated value with the second file validity data in the third file; and

determining whether the second file is valid based on the comparing of the second file calculated value with the second file validity data in the third file; and

executing the application data on the communication device if the application data is verified using the application validity data in the second file and if it is determined that the second file is valid.

2. (Canceled)

3. (Canceled)

4. (Canceled)
5. (Canceled)
6. (Canceled)
7. (Previously Presented) The communication device of claim 1, wherein, if it is determined that the second file is valid, the processor further verifies whether the application data in the first file is valid using the application validity data in the second file.
8. (Previously Presented) The communication device of claim 7, where the application validity data is calculated on the basis of a one-way application validity function, the one-way application validity function using at least a part of the application data in the first file to generate the application validity data.
9. (Previously Presented) The communication device of claim 8, where the one-way application validity function comprises a hash function;
where the application validity data comprises a hash value;
where at least a part of the first file is input to the hash function to generate a calculated hash value; and
where using the application validity data in the second file to verify the validity of the application data in the first file comprises comparing the calculated hash value with the hash value in the second file.
10. (Previously Presented) The communication device of claim 9, where the one-way application validity function and the one-way function each comprise the same hash function.
11. (Previously Presented) The communication device of claim 1, where the application data comprises an application program.

12. (Previously Presented) The communication device of claim 1, where at least a part of the second file comprises independent data, the independent data being independent of the application data contained in the first file; and

where generating a second file calculated value using the one-way function comprises inputting the independent data to the one-way function to generate the second file calculated value.

13. (Previously Presented) The communication device of claim 12, where the independent data comprises certificate data for certifying authenticity of the application data, the certificate data being provided by a certificate authority.

14. (Previously Presented) The communication device of claim 13, where the third file is received from a trusted server;

where the second file is received from a content provider server, the content provider server being different from the trusted server; and

where the third file is used to verify the certificate data in the second file.

15. (Previously Presented) The communication device of claim 1, where the one-way function comprises a hash function;

where the second file validity data comprises a hash value;

where at least a part of the second file is input to the hash function to generate a calculated hash value; and

where comparing the second file calculated value with the second file validity data in the third file comprises comparing the calculated hash value with the hash value in the third file.

16. (Previously Presented) The communication device of claim 1, where the receiver receives the second and third files prior to receiving the first file; and

where the receiver receives the first file only after the at least one processor determines whether the second file is valid.

17. (Canceled)

18. (Currently Amended) A method for a communication device to verify whether application data is valid in order to determine whether to execute the application data on the communication device, the verification of the application data using a first file, a second file, and a third file, the first file comprising the application data, the second file comprising application validity data used to verify validity of the application data in the first file and containing data indicating a location where a program, which is contained in the first file and run in the communication device, is stored, the first file, second file, and the third file being separate from one another, the third file comprising second file validity data calculated with a one-way function and used to verify the second file, the method comprising:

receiving the first file, the second file and the third file at the communication device,
generating a second file calculated value using the one-way function, at least a part of the second file being input to the one-way function to generate the second file calculated value;
comparing the second file calculated value with the second file validity data in the third file;

determining whether the second file is valid based on the comparing of the second file calculated value with the second file validity data in the third file; and

executing the application data on the communication device if the application data is verified using the application validity data in the second file and if it is determined that the second file is valid.

19. (Previously Presented) The method of claim 18, further comprising, if it is determined that the second file is valid, verifying whether the application data in the first file is valid using the application validity data in the second file.

20. (Previously Presented) The method of claim 19, where the application validity data is calculated on the basis of a one-way application validity function, the one-way application validity function using at least a part of the application data in the first file to generate the application validity data.

21. (Previously Presented) The method of claim 20, where the one-way application validity function comprises a hash function;

where the application validity data comprises a hash value;

where at least a part of the first file is input to the hash function to generate a calculated hash value; and

where using the application validity data in the second file to verify the validity of the application data in the first file comprises comparing the calculated hash value with the hash value in the second file.

22. (Previously Presented) The method of claim 21, where the one-way application validity function and the one-way function each comprise the same hash function.

23. (Previously Presented) The method of claim 18, where the application data comprises an application program.

24. (Previously Presented) The method of claim 18, where at least a part of the second file comprises independent data, the independent data being independent of the application data contained in the first file; and

where generating a second file calculated value using the one-way function comprises inputting the independent data to the one-way function to generate the second file calculated value.

25. (Previously Presented) The method of claim 24, where the independent data comprises certificate data for certifying authenticity of the application data, the certificate data being provided by a certificate authority.

26. (Previously Presented) The method of claim 25, where the third file is received from a trusted server;

where the second file is received from a content provider server, the content provider server being different from the trusted server; and

where the third file is used to verify the certificate data in the second file.

27. (Previously Presented) The method of claim 18, where the one-way function comprises a hash function;

where the second file validity data comprises a hash value;

where at least a part of the second file is input to the hash function to generate a calculated hash value; and

where comparing the second file calculated value with the second file validity data in the third file comprises comparing the calculated hash value with the hash value in the third file.

28. (Previously Presented) The method of claim 18, where the second and third files are received prior to receiving the first file; and

where the first file is received only after determining whether the second file is valid.

29. (Canceled)